



Department of Computer Science
MSc Data Communications, Networks & Distributed Systems

ZION

A Lightweight SEINIT based Security Framework Implementation for Pervasive Computing

System & User Manual

September 2004

Team X-Matrix

Kumardev Chatterjee

Philip Ho

Wasif Mehdi

Fahd Shariff

Muhammad Solangi

Supervisor

Steve Hailes

This report is submitted as part requirement of the MSc Degree in Data Communications, Networks and Distributed Systems at University College London. It is substantially the result of our own work except where explicitly indicated in the text.

The report may be freely copied and distributed provided the source is explicitly acknowledged.

APPENDIX A: System Manual

This document contains all the technical details such as how the system should be compiled and run. It also describes where the code is stored so that it can be modified in the future.

The official homepage of this project is:

http://www.cs.ucl.ac.uk/students/z15_1

All documents and code may be downloaded from here.

A.1 System Requirements

- This software requires Java 2 version 1.3 or 1.4. Before installing make sure you have a compatible Java virtual machine.
- The recommended operating system is Red Hat Linux.
- You will need approximately 5.13 MB of free disk space to complete the installation on your hard disk, although the software can also be run directly from the CD provided.

A.2 Installation Instructions

- Insert the CD provided into your CD-ROM drive.
- The CD contains the following files and folders:
 - `src` which contains all the software code, libraries and compiled binaries,
 - `docs` which contains PDF versions of the Group project documents, and
 - `README.txt` which explains the contents of the CD, the directory structure and these instructions.
- Installation complete!

A.3 Launching the Security Framework

- Change to the `src` directory: `cd src/`
- On UNIX-based systems (Recommended):
 - Start the framework by typing `runit` in your favourite shell. You will see output on the terminal window describing the components being registered and started. Finally you will see the Audit Tool display window.
- On Windows:
 - Double click on `runreg.bat` or type `runreg.bat` at the command prompt. This will register the components.
 - Double click on `runit.bat` or type `runit.bat` at the command prompt. This will start up the Security Manager and will display the Audit Tool.
- The Security Framework is now up and running!

A.4 Running the Sample Chat Application

A sample chat application has been provided in the `demoapps` package. Launch this application by typing:

```
java demoapps.ChatInterface
```

A chat window will be displayed. All text entered in this window will be encrypted by the Zion based on the current context.

A.5 For Developers

The `src` directory contains all the source code, java class libraries and compiled binaries. It also contains the following files and folders:

- **`.project`** and **`.classpath`**: These files define the project and buildpath settings for Eclipse, which was the Java Development Environment used to build the entire system. Hence the system can be *imported* directly into Eclipse and worked on.
- **`runit`**: A shell script which sets the classpath and runs the `ComponentRegistrar` and `SecurityManager`.
- **`runreg.bat`** and **`runit.bat`**: These are Windows batch files which run the `ComponentRegistrar` and `SecurityManager` respectively.

- **SEINIT.txt**: Defines port numbers for application types.
- **examplePolicies**: This directory contains the Ponder security policy (policy.pol), XML security policy (policy.xml) and the XML context representation (context-eg.xml).
- **satIn.jar**: All SATIN source code is present in java archive lib/satIn.jar.

APPENDIX B: User Manual

This document aims to provide help and assistance to users of Zion. The purpose of the framework is to dynamically enforce new security measures when context changes.

The system includes an Audit Tool which is used for inspecting the state of the system at any point in time and for observing the messages being passed between its various components. The Audit Tool also includes a Context Dialog for triggering context change events. In addition, the “replay” feature is useful for inspecting past sessions.

The sections below cover basic usage of the different features provided by the Audit Tool.

B.1 Audit Message Display

The top half of the Audit Tool displays messages describing what is going on in the system. It is divided into a Master Pane on the left and a set of Component Panes on the right. The Master Pane displays main messages of the entire system, whereas the individual component panes display what each component is doing. All messages are preceded by the time they were generated and the time of display.

B.2 Adding and Removing Message Panes

Individual message panes can be added and removed from the display window by going into the View menu and (de)selecting the pane that you wish to be added or removed.

B.3 State Transition Diagram

The diagram in the bottom half of the main window is called the *state transition diagram* for the system. It shows the states that the system can be in at any time and the transitions between allowable states. These transitions are triggered by events which are labelled on the transition arrows.

As events take place, state transitions can be observed. The current state and transition is represented in red to distinguish it from other parts of the diagram.

B.4 Resizing the State Transition Diagram

The diagram can be resized using the following:

- **Keyboard:** The arrow keys on the keyboard can be used to compress horizontally (←), compress vertically (↑), expand horizontally (→) and expand vertically (↓).
- **Menu:** The STD menu displays items for resizing the diagram.
- **Toolbar:** The STD toolbar can be selected via the STD menu. The toolbar docks itself in the diagram window and holds buttons for resizing the diagram.

B.5 Removing the State Transition Diagram

The diagram can be removed by going into the View menu and deselecting the STD option. It can be added again by selecting the STD option.

B.6 Changing Context

The Context Dialog can be accessed through Menu → File → Input Context. The dialog holds two tabs, one for inputting context and the other for displaying the XML representation for that context.

Context can be changed by selecting a different device, network connection and/or location from the drop down boxes present on the dialog. Pressing the *Apply* button triggers a context change event and the system responds accordingly.

B.7 Replaying Past Sessions

By default, the Audit Tool writes all displayed messages to a log file. This log file can be specified as an argument to the Security Manager before it is run. The *replay* function allows you to load a previous log session's messages into the Audit Display.

This is done via Menu → File → Open and then selecting the log file that you wish to be replayed from the File Dialog box. After pressing *OK*, the Audit Display is populated with messages from the selected log file.

B.8 Getting Help

The Help menu displays help information for the Audit Tool and the State Transition Diagram.

B.9 Exiting the System

The system can be exited by Menu → File → Exit.